

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2006-261850

(P2006-261850A)

(43) 公開日 平成18年9月28日(2006.9.28)

(51) Int. Cl.	F I	テーマコード (参考)
H04L 12/28 (2006.01)	H04L 12/28 300A	5K033
	H04L 12/28 310	

審査請求 未請求 請求項の数 12 O L (全 17 頁)

(21) 出願番号 特願2005-73951 (P2005-73951)
 (22) 出願日 平成17年3月15日 (2005.3.15)

(71) 出願人 000001007
 キヤノン株式会社
 東京都大田区下丸子3丁目30番2号
 (74) 代理人 100076428
 弁理士 大塚 康德
 (74) 代理人 100112508
 弁理士 高柳 司郎
 (74) 代理人 100115071
 弁理士 大塚 康弘
 (74) 代理人 100116894
 弁理士 木村 秀二
 (72) 発明者 井戸 哲男
 東京都大田区下丸子3丁目30番2号 キ
 ヤノン株式会社内

最終頁に続く

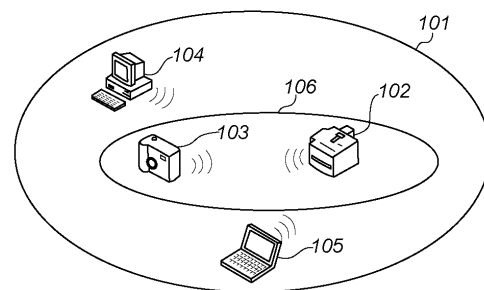
(54) 【発明の名称】 通信装置及びそのネットワーク構築方法

(57) 【要約】

【課題】 通信装置間で構築されるネットワークにおいて、第三者からの不正なアクセスを防ぐと共に、第三者からの影響による通信速度の低下を防ぐ。

【解決手段】 ネットワークの識別子を隠蔽した報知信号を送信する機能を有する通信装置において、他の通信装置との間でネットワークを構築する際に、特定の通信装置とネットワークを構築したか否かを判定し、ネットワークを構築したと判定した場合に、ネットワークの識別子を隠蔽した報知信号を発信する。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

ネットワークの識別子を隠蔽した報知信号を送信する機能を有する通信装置であって、他の通信装置との間でネットワークを構築する際に、特定の通信装置とネットワークを構築したか否かを判定する判定手段と、

前記判定手段でネットワークを構築したと判定した場合に、前記ネットワークの識別子を隠蔽した報知信号を発信する手段とを有することを特徴とする通信装置。

【請求項 2】

前記判定手段は、他の通信装置を特定するための情報に基づいて前記特定の通信装置とネットワークを構築したか否かを判定することを特徴とする請求項 1 記載の通信装置。

10

【請求項 3】

前記判定手段は、前記ネットワークを構築すべき通信装置の台数を示す情報に基づいて前記特定の通信装置とネットワークを構築したか否かを判定することを特徴とする請求項 1 記載の通信装置。

【請求項 4】

前記報知信号を発信した後、前記ネットワークの識別子とは異なる識別子を暗号化して通信することを特徴とする請求項 1 記載の通信装置。

【請求項 5】

前記報知信号を発信した後、前記特定の通信装置との間で前記ネットワークの識別子とは異なる識別子を生成して通知することを特徴とする請求項 1 記載の通信装置。

20

【請求項 6】

前記報知信号を発信した後、前記特定の通信装置との間で前記ネットワークの識別子とは異なる識別子を共有することを特徴とする請求項 1 記載の通信装置。

【請求項 7】

前記ネットワークの識別子で構築されていたネットワークを切断し、前記異なる識別子を用いて新たなネットワークを構築することを特徴とする請求項 4 乃至 6 の何れか一項に記載の通信装置。

【請求項 8】

前記異なる識別子を用いて構築したネットワークを切断し、元のネットワークの識別子を用いてネットワークに参加することを特徴とする請求項 7 記載の通信装置。

30

【請求項 9】

前記ネットワークに参加する際に、通信装置を特定する情報を設定し直すことを特徴とする請求項 8 記載の通信装置。

【請求項 10】

ネットワークの識別子を隠蔽した報知信号を送信する機能を有する通信装置のネットワーク構築方法であって、

他の通信装置との間でネットワークを構築する際に、特定の通信装置とネットワークを構築したか否かを判定する判定工程と、

前記判定工程でネットワークを構築したと判定した場合に、前記ネットワークの識別子を隠蔽した報知信号を発信する工程とを有することを特徴とする通信装置のネットワーク構築方法。

40

【請求項 11】

請求項 10 記載の通信装置のネットワーク構築方法をコンピュータに実行させるためのプログラム。

【請求項 12】

請求項 11 記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】**【技術分野】****【0001】**

本発明は、ネットワークの識別子を隠蔽した報知信号を送信する機能を有する通信装置

50

及びそのネットワーク構築方法に関するものである。

【背景技術】

【0002】

従来、複数の無線端末装置がお互いに無線通信を行う「アドホックモード」と呼ばれる無線LANシステムが提供されている。このような無線LANシステムでは、2台の無線端末装置（以下、一方をクリエータの役割を持つ「ステーションA」、他方をジョイナーの役割を持つ「ステーションB」という）との間で通信を確立するには、ステーションAから常時一定周期で、SSID（Service Set Identifier、サービス・セット識別子）を含むビーコン情報を報知信号として周囲に発信することにより、そのビーコン情報を受信したステーションBがビーコン情報に含まれているSSIDを使用してステーションAとの通信の確立を行うことが最も一般的な方法である。 10

【0003】

一方、ビーコン情報に含まれるSSIDを隠蔽することにより、ネットワーク上からステーションAの存在を隠し、ステーションAのSSIDを予め知っているユーザしか接続できない「ステルスモード機能」を有するステーションも存在する。

【0004】

また、アクセスポイント装置（以下、「AP」という）と複数の無線端末装置（以下、「STA」という）との間で無線通信を行う「インフラストラクチャモード」と呼ばれる無線LANシステムも提供されている。この無線LANシステムでも、上述のアドホックモードと同様に、クリエータとしてのAPから常時一定周期で、SSIDを含むビーコン情報を周囲に発信することにより、STAがビーコン情報に含まれているSSIDを使用して他のSTAとの通信の確立を行うことが最も一般的な方法である。 20

【0005】

また、インフラストラクチャモードでも、上述したビーコン情報に含まれるSSIDを隠蔽する「ステルスモード機能」を有するAPも存在する（例えば、特許文献1参照）。この特許文献1には、ステルス機能を持つAPが、SSIDをブランクで接続を試みるSTAからの接続を拒否することが開示されている。

【特許文献1】特開2004 - 32133号公報

【発明の開示】

【発明が解決しようとする課題】

30

【0006】

しかしながら、上述したステルス機能を使用しない最も一般的な無線通信を行う従来の無線LANシステムでは、SSIDがネットワーク上で公開されてしまうため、ネットワーク上の誰でもSSIDを読み取ることができる。そのため、任意の第三者が不正なアクセスをしてくる可能性が高くなってしまい、セキュリティ面で好ましくない。また、それが原因で無線通信の転送速度を下げてしまう。

【0007】

更に、ステルス機能を使用したとしても、一度無線接続を行ったユーザにとっては既にSSIDを認識しているため、たとえステルス機能を使用したとしても、無線端末同士の一対一接続に参加を試みるのが可能であり、またそれが原因で無線通信の転送速度を下げることは避けることができない。 40

【0008】

本発明は、上述の事情に鑑みてなされたもので、通信装置間で構築されるネットワークにおいて、第三者からの不正なアクセスを防ぐと共に、第三者からの影響による通信速度の低下を防ぐことを目的とする。

【課題を解決するための手段】

【0009】

本発明は、ネットワークの識別子を隠蔽した報知信号を送信する機能を有する通信装置であって、他の通信装置との間でネットワークを構築する際に、特定の通信装置とネットワークを構築したか否かを判定する判定手段と、前記判定手段でネットワークを構築した 50

と判定した場合に、前記ネットワークの識別子を隠蔽した報知信号を発信する手段とを有する。

【0010】

また、本発明は、ネットワークの識別子を隠蔽した報知信号を送信する機能を有する通信装置のネットワーク構築方法であって、他の通信装置との間でネットワークを構築する際に、特定の通信装置とネットワークを構築したか否かを判定する判定工程と、前記判定工程でネットワークを構築したと判定した場合に、前記ネットワークの識別子を隠蔽した報知信号を発信する工程とを有することを特徴とする。

【発明の効果】

【0011】

本発明によれば、通信装置間で構築されるネットワークにおいて、第三者からの不正なアクセスを防ぐことが可能となると共に、第三者からの影響による通信速度の低下を防ぐことが可能となる。

【発明を実施するための最良の形態】

【0012】

以下、図面を参照しながら発明を実施するための最良の形態について詳細に説明する。

【0013】

〔第1の実施形態〕

図1は、第1の実施形態における無線LANシステムの構成例を示す図である。図1において、101はIEEE 802.11b/a/g準拠の無線LANシステムにおけるアドホックネットワークを構成可能な範囲である。102は無線LANに対応し、プリンタ、ファクシミリ、スキャナ、或いはこれらの機能を複合したマルチファンクションシステム（無線LAN機能を備えた無線端末装置）である。また、無線端末装置102は、例えば子局としての機能及び親局（制御局）としての機能をそれぞれ備えているものとする。

【0014】

尚、第1の実施形態では、無線端末装置102は親局として機能し、後述する103、104、105に示す無線端末が子局として機能するものとする。

【0015】

103は無線LAN機能を備えたデジタルカメラなどの無線端末装置であり、撮像した画像のファイルを無線接続により無線端末装置102へ転送する。104は無線LAN機能を備えたパーソナルコンピュータなどの無線端末装置であり、文書ファイルを無線接続により無線端末装置102へ転送するか、或いは無線端末装置102で読み取った原稿のファイルを無線接続により読み込む。105は無線LAN機能を備えたノート型パソコンなどの無線端末装置である。

【0016】

また、無線端末装置102は、自身に接続可能な無線端末の情報として、無線端末装置103、104のMACアドレスを予め所有している。その上で、無線端末装置102は、常時一定周期で、ドメインID（SSID）を含むビーコン信号をアドホックネットワーク上の全ての無線端末装置103、104、105に対して送る。このビーコン信号に対して無線端末装置103、104、105は、自らも備えているIDを含む信号を無線端末装置102に対して接続要求として送る。そして、この場合、MACアドレスとSSIDとの両者が一致している無線端末装置（この例では、無線端末装置103、104）に対してだけ接続を許可し、特定のデータ通信の準備を行う。即ち、SSID以外に設定されたMACアドレスの一致／不一致に基づいて接続の可否を決定する。

【0017】

ここで、第1の実施形態において、無線端末装置102と無線端末装置103との間で特定のデータ通信チャネル106が確立するまで（即ち、データリンクが確立するまで）の接続時の手順について、図1乃至図4を用いて説明する。

【0018】

図2は、無線端末装置間における接続時のシーケンスを示す図である。また、図3は、

10

20

30

40

50

第 1 の実施形態における接続時の処理を示すフローチャートである。更に、図 4 は、第 1 の実施形態における無線端末装置 102 の概略構成を示すブロック図である。尚、図 4 には、無線端末装置 102 の通信部のみを示しているが、装置全体を制御する制御部や上述した複数の機能を実現する複数の機能部などが含まれるのは言うまでもない。この点は、他の実施形態においても同様である。

【0019】

まず、クリエイタとしての無線端末装置 102 がドメイン ID (SSID) を含むビーコン信号をアドホックネットワーク上の全ての無線端末装置 103、104、105 に対して発信する (201、S301)。次に、このビーコン信号を受信した各無線端末装置から接続要求信号の受信を待つ (S302)。そして、無線端末装置 103、104、105 から送信元端末識別情報 (例えば、MAC アドレス) を含む接続要求信号をそれぞれ受信すると (S302 の YES)、その送信元端末識別情報が図 4 に示す無線端末装置 102 の無線端末情報記憶部 401 に予め登録しておいた情報 (例えば、無線端末装置 103、104 の MAC アドレス) と一致するか否かを確認する (S303)。

10

【0020】

ここで、送信元端末識別情報が無線端末情報 (401) と一致しなければ (S303 の NO)、接続要求を破棄し、次の接続要求に備える。また、送信元端末情報が無線端末情報 (401) と一致すれば (S303 の YES)、無線端末装置 102 から無線端末装置 103、104 へ接続要求信号の返信を行う (S304)。

【0021】

次に、無線端末装置 102 と無線端末装置 103、104 との間で認証シーケンス処理が行われ (S305)、認証シーケンスが完了すると、アソシエーション処理が行われる (202、S306 ~ S309)。ここで、無線端末装置 102 は無線端末装置 103、104 間で特定のデータ通信チャネルが確立すると、無線端末装置 102 からアドホックネットワークを構成可能な範囲 101 内の無線端末装置 103、104、105 に対して発信していた SSID を含むビーコン信号を SSID を含まないビーコン信号に切り替える、即ちステルスモードに移行する (203、S310)。これにより、アドホックネットワークを構成可能な範囲 101 内から無線端末装置 102 の存在を隠す。

20

【0022】

これ以降、無線端末装置 102 と無線端末装置 103、104 間でデータ通信が可能となり (S311)、他の無線端末装置 (図 1 に示す例では、無線端末装置 105) が無線端末装置 102 のアドホックネットワークへ参加することが不可能となる。

30

【0023】

尚、無線端末装置 102 の無線端末情報記憶部 401 に登録しておく情報は、装置内の不揮発性メモリに保持し、任意に書き換え可能なものでも良いし、或いは工場出荷時に、ROM に書き込まれ、その後、書き換えができないものでも良い。

【0024】

第 1 の実施形態によれば、通信装置間で構築されるネットワークにおいて、特定の通信装置からの参加を防止し、セキュリティを向上させることができる。

【0025】

40

[第 2 の実施形態]

次に、図面を参照しながら本発明に係る第 2 の実施形態について詳細に説明する。第 2 の実施形態では、無線 LAN の機能を有し、プリンタ、ファクシミリ、スキャナ、それらの機能を複合したマルチファンクションシステムなどの無線端末装置 (親機) と、これに接続することを許可されている無線端末装置群 (子機) との間で特定データ通信チャネルを確立させて通信を行う無線 LAN システムにおいて、無線端末装置に対して接続した、無線端末装置群の内、任意の無線端末装置 (子機) の台数が、当該無線端末装置 (親機) に予め設定した台数に達するまでは従来技術で最も一般的な手法を採用し、SSID をネットワーク上に公開する。その上で、予め設定した台数に達したときに、その SSID をステルス化することで、任意の第三者が当該無線端末装置 (親機) と任意の無線端末装置 (子機)

50

との間で確立された特定データ通信チャネルに進入してくることを困難にする無線LANシステムを提供するものである。

【0026】

尚、第2の実施形態における無線LANシステムの構成は、図1を用いて説明した第1の実施形態の構成と同様であり、その説明は省略する。

【0027】

ここで、無線端末装置102と無線端末装置103との間で特定のデータ通信チャネルが確立するまで（即ち、データリンクが確立するまで）の第2の実施形態における接続時の手順について、図2、図5、図6を用いて説明する。

【0028】

図5は、第2の実施形態における接続時の手順を示すフローチャートである。図6は、第2の実施形態における無線端末装置102の概略構成を示すブロック図である。

【0029】

まず、クリエータとしての無線端末装置102がドメインID（SSID）を含むビーコン信号をアドホックネットワーク上の全ての無線端末装置103、104、105に対して発信する（201、S501）。次に、このビーコン信号を受信した各無線端末装置から接続要求信号の受信を待つ（S502）。そして、無線端末装置103、104、105から送信元端末識別情報（例えば、MACアドレス）を含む接続要求信号をそれぞれ受信すると（S502のYES）、接続要求信号を受信した無線端末装置の台数が、予め設定した台数（図6に示す接続端末台数記憶部601に記憶されている台数）に達したか否かを判定する（S503）。ここで、記憶部601に設定された台数を越えた場合、以降の接続要求を破棄し、ステップS501に戻る。記憶部601に設定された台数を越えない場合、無線端末装置102から無線端末装置103、104へ接続要求信号の返信を行う（S504）。

【0030】

次に、第1の実施形態と同様に、無線端末装置102と無線端末装置103、104との間で認証シーケンス処理が行われ（S505）、認証シーケンスが完了すると、アソシエーション処理が行われる（202、S506～S509）。ここで、無線端末装置102は無線端末装置103、104間で特定のデータ通信チャネルが確立すると、無線端末装置102からアドホックネットワークを構成可能な範囲101内の無線端末装置103、104、105に対して発信していたSSIDを含むビーコン信号をSSIDを含まないビーコン信号に切り替える、即ちステルスモードに移行する（203、S510）。これにより、アドホックネットワークを構成可能な範囲101内から無線端末装置102の存在を隠す。

【0031】

これ以降、無線端末装置102と無線端末装置103、104間でデータ通信が可能となり（S511）、他の無線端末装置（図1に示す例では、無線端末装置105）が無線端末装置102のアドホックネットワークへ参加することが不可能となる。

【0032】

尚、図6に示す接続端末台数記憶部601に予め設定してある台数は、不揮発性メモリに保持し、任意に書き換え可能なものでも良いし、或いは工場出荷時にROMに書き込まれ、その後、書き換えができないものでも良い。

【0033】

第2の実施形態によれば、無線端末装置に対して接続する無線端末装置が予め設定した台数に達したときに、データ通信サービスを楽しむための準備（機密保護手段）である認証又は加入などの手順で使用されるSSIDをステルス化するので、セキュリティを高めることができる。

【0034】

[第3の実施形態]

次に、図面を参照しながら本発明に係る第3の実施形態について詳細に説明する。第2

10

20

30

40

50

の実施形態では、無線LANシステムが有するSSIDは予め設定した台数までネットワーク上に公開されているため、SSIDをステルス化した後も、先のSSIDを理解した任意の第三者が存在した場合、その任意の第三者が、無線端末装置に対して不正なアクセスをしてくる可能性も否定できない。

【0035】

そこで、第3の実施形態では、SSIDをステルス化した後、先のSSIDと異なるSSIDを無線端末装置（親機）と任意の無線端末装置（子機）との間で確立された特定データ通信チャネルを使用して、無線端末装置（親機）から、暗号化してユニキャストで送信し、異なるSSIDを用いて再度無線端末装置（親機）と任意の無線端末装置（子機）との間で、新しい特定のデータ通信チャネルを確立することにより、任意の第三者が新しい特定データ通信チャネルに進入してくることを防ぐ無線LANシステムを提供するものである。

【0036】

第3の実施形態における無線LANシステムの構成は、上述した第2の実施形態の構成と同様であり、その説明は省略する。

【0037】

図7は、第3の実施形態における無線端末装置間のシーケンスを示す図である。第3の実施形態では、図1に示す無線端末装置102がクリエータとして動作し、無線端末装置102と特定のデータ通信チャネル106を確立した無線端末装置103がジョイナー（Joiner）として動作する。

【0038】

図8は、第3の実施形態におけるデータ通信可能後の処理を示すフローチャートである。まず、図5に示した第2の実施形態における通信チャネル確立処理を行い（S801）、その後、無線端末装置102と無線端末装置103とが、同じアプリケーションを動作させているとき、このアプリケーションにより、通信チャネル106を確立するのに使用したSSIDとは異なるSSIDを作成し（S802）、作成したSSIDを暗号化したものを、既に確立している通信チャネル106を使用してユニキャストで無線端末装置103に対して送信する（704、S803）。

【0039】

尚、異なるSSIDは、アプリケーション自体が作成しても良いし、図9に示すSSID記憶部901に予め設定しておいても良い。

【0040】

そして、無線端末装置103上で動作しているアプリケーションは、暗号化されたSSIDを受信すると、受信完了したことを示す情報を無線端末装置102に返信する（705、S804）。その後は、互いに通知しあった新規のSSIDに変更し、このSSIDを用いて無線端末装置102と無線端末装置103との間で、新しいデータ通信チャネルを確立する。

【0041】

第3の実施形態によれば、第2の実施形態に比べて更にセキュリティを向上させることができる。

【0042】

[第4の実施形態]

次に、図面を参照しながら本発明に係る第4の実施形態について詳細に説明する。第4の実施形態では、ステルスモードにおいて新しい特定のデータ通信チャネルで異なるSSIDを使用することで、異なるSSIDを無線端末装置（親機）と無線端末装置（子機）とにしかわからないものとし、任意の第三者にSSIDを読み取られる恐れのないセキュリティの高い無線LANシステムを提供するものである。

【0043】

第4の実施形態における無線LANシステムの構成は、上述した第3の実施形態の構成と同様であり、その説明は省略する。

【0044】

第4の実施形態について図10乃至図12を用いて説明する。図10は、第4の実施形

10

20

30

40

50

態における無線端末装置間のシーケンスを示す図である。図 1 1 は、第 4 の実施形態における処理を示すフローチャートである。図 1 2 は、第 4 の実施形態における無線端末装置 1 0 2 の概略構成を示すブロック図である。

【 0 0 4 5 】

第 3 の実施形態と同様に、SSIDがステルス化され、通信チャネル確立処理が行われた後 (1 0 0 1 ~ 1 0 0 3、S 1 1 0 1)、無線端末装置 1 0 2 と無線端末装置 1 0 3 とが、同じアルゴリズムを使用してSSIDとは異なるSSIDを作成する。具体的には、作成するSSIDは、先のSSIDに基づいて確立した通信チャネルを用いて受信したデータから通信相手特有の情報を取得し (S 1 1 0 2)、その情報と、無線端末装置 1 0 2 及び 1 0 3 に予め設定してある情報とを組み合わせ (S 1 1 0 3)、新たなSSIDを作成する (S 1 1 0 4)。 10
そして、SSID作成完了通知をユニキャストで行う (1 0 0 4、S 1 1 0 5)。

【 0 0 4 6 】

その後、通信相手からSSID作成完了通知を受信すれば (1 0 0 5、S 1 1 0 6)、作成したSSIDをお互いに共有したとみなすことができる。そして、互いに共有した新規のSSIDに変更し、このSSIDを用いて無線端末装置 1 0 2 と無線端末装置 1 0 3 との間で、新しいデータ通信チャネルを確立する。このとき、予め無線端末装置 1 0 2 及び 1 0 3 に設定してある情報 (図 1 2 に示すSSID作成部 1 2 0 2 の情報は) 自身のMACアドレスやIPアドレスといった情報が考えられる。

【 0 0 4 7 】

また、無線端末装置 1 0 2 が受信データから取得する固有情報 (1 2 0 2) には、通信 20
相手固有の情報であるMACアドレスやIPアドレスなどが考えられる。また、これらの情報は、当該無線通信機能が備える不揮発性メモリに保持し、任意に書き換え可能なものである。

【 0 0 4 8 】

第 4 の実施形態によれば、第 3 の実施形態に比べて更にセキュリティを向上させることができる。

【 0 0 4 9 】

[第 5 の実施形態]

次に、図面を参照しながら本発明に係る第 5 の実施形態について詳細に説明する。第 5
の実施形態では、特定データ通信チャネルを確立したとき、確立した特定データ通信チャ 30
ネルでは通信サービスを行わず、データ通信チャネルとは異なるSSIDを通知し、そのSSIDを共有する無線端末装置との間で新しい通信ネットワークを構築するものである。

【 0 0 5 0 】

図 1 3 は、第 5 の実施形態における無線LANシステムの構成例を示す図である。図 1
3 において、1 3 0 1 はデータ通信チャネル 1 0 6 とは異なる特定のデータ通信チャネル
である。その他の構成については、図 1 に示した構成と同じであり、同じ符号を付与して
その説明は省略する。

【 0 0 5 1 】

ここで、第 5 の実施形態において、無線端末装置 1 0 2 と無線端末装置 1 0 3 との間で
特定データ通信チャネル 1 3 0 1 が確立するまで (即ち、データリンクが確立するまで) 40
の接続時の手順について、図 1 3 乃至図 1 5 を用いて説明する。

【 0 0 5 2 】

図 1 4 は、第 5 の実施形態におけるシーケンスを示す図である。また、図 1 5 は、第 5
の実施形態における処理を示すフローチャートである。

【 0 0 5 3 】

第 5 の実施形態では、第 1 又は第 2 の実施形態と同様に無線端末装置 1 0 2 と無線端末
装置 1 0 3 とがSSID1を使用してアソシエーション処理を行い (1 4 0 1、1 4 0 2)、
そのSSID1をステルス化した後 (1 4 0 3)、第 3 又は第 4 の実施形態と同様に、SSID1と
は異なるSSID2を共有する (1 4 0 4)。そして、一旦、先のSSID1に基づく通信チャネル
1 0 6 を切断し (1 4 0 5)、ネットワーク上で両者だけが共有しているSSID2を用いて 50

新しい通信チャネル 1301 を確立する (1406 ~ 1408)。

【 0054 】

尚、無線端末装置 102 は発信するビーコン情報に SSID2 を含まないステルスモードを使用して新しい通信チャネル 1301 を確立するものとする。

【 0055 】

ここで、無線端末装置 102 と無線端末装置 103 との新しい特定データ通信チャネルを確立するまでの接続時の処理について、図 15 を用いて説明する。

【 0056 】

図 15 は、第 5 の実施形態における処理を示すフローチャートである。まず、無線端末装置 102 が特定データ通信チャネル 106 の確立処理を行い (S 1501)、無線端末装置 103 へ暗号化した SSID2 を送信する (S 1502)。そして、無線端末装置 103 から SSID2 受信完了通知を受信し (S 1503)、SSID2 を共有した状態で、無線端末装置 102 に予め設定した時間が経過すると、自動的に SSID1 を用いて確立した通信チャネルを切断する (S 1504)。

【 0057 】

その後、改めて共有した SSID2 を含まないビーコンをステルスモードで発信し (S 1505)、接続要求信号を送信してきた無線端末装置に対して新しい通信チャネル 1301 を確立する処理を実行する (1506 ~ 1509) を行う。

【 0058 】

第 5 の実施形態によれば、無線端末装置との間で通信されるデータの機密が漏洩することを防ぐことができ、且つ無線端末装置と確立した特定のデータ通信チャネルに第三者の侵入を防ぐことが可能となる。これにより、各々の通信チャネルにサービスの内容を限定することが可能となるため、様々な使用形態に発展させることができる。

【 0059 】

[第 6 の実施形態]

次に、図面を参照しながら本発明に係る第 6 の実施形態について詳細に説明する。第 6 の実施形態では、異なる SSID を使用して無線端末装置 (親機) と無線端末装置群 (子機) とで形成した新しいネットワークから、無線端末装置群の任意の無線端末装置が退出した場合、即ち予め設定した接続台数より少なくなった場合、無線端末装置はステルスモードを解除し、再度元の SSID をネットワーク上に公開する無線 LAN システムを提供するものである。

【 0060 】

図 16 は、第 6 の実施形態における無線 LAN システムの構成例を示す図である。図 16 において、1601 は無線無線端末装置 102 によるアドホックネットワークの範囲で、図 13 に示す通信チャネル 106 又は新たな通信チャネル 1301 である。1602 は参加していたアドホックネットワーク 1601 から外れた無線端末装置である。その他の構成については図 1 と同じであり、同じ符号を付与し、その説明は省略する。

【 0061 】

図 17 は、第 6 の実施形態における無線端末装置のシーケンスを示す図である。図 17 に示すように、無線端末装置 102 が SSID1 を含むビーコンを送信し (1701)、アソシエーション処理を行い (1702)、SSID1 をステルス化し (1703)、データ通信可能となる (1704)。

【 0062 】

この状態において、無線端末装置 103 が参加していた通信チャネル 1601 から抜け出した場合、無線端末装置 102 はその通信チャネル 1601 を切断する (1705)。そして、SSID1 を含むビーコンを無線端末装置群に対して発信する (1706)。

【 0063 】

また、図 18 は、第 6 の実施形態における無線端末装置の他のシーケンスを示す図である。このシーケンスは、図 16 に示すアドホックネットワークの範囲 1601 が SSID2 で構成された通信チャネル 1301 であった場合のシーケンスである。

【 0 0 6 4 】

ここで、図 1 8 に示す 1 8 0 1 ~ 1 8 0 7 までは、図 1 4 に示す 1 4 0 1 ~ 1 4 0 8 と同様であり、その説明は省略する。

【 0 0 6 5 】

上述したように、データ通信が可能な状態になり、無線端末装置 1 0 3 が参加していた通信チャネル 1 6 0 1 から抜け出した場合、無線端末装置 1 0 2 はその通信チャネル 1 6 0 1 を切断する (1 8 0 8)。そして、SSID1を含むビーコンを無線端末装置群に対して発信する (1 8 0 9)。

【 0 0 6 6 】

尚、第 6 の実施形態では、無線端末装置 1 0 3 がアドホックネットワークから退出した場合を例に説明したが、無線端末装置 1 0 2 がアドホックネットワークを退出した場合も適用できることは言うまでもない。

【 0 0 6 7 】

第 6 の実施形態によれば、無線端末装置がアドホックネットワークから退出したときに新しく構築したネットワークを切断し、元のネットワークを再構築することにより、無線端末装置が自動的に元のネットワークに再参加することが可能となる。

【 0 0 6 8 】

[第 7 の実施形態]

次に、図面を参照しながら本発明に係る第 7 の実施形態について詳細に説明する。第 7 の実施形態では、無線端末装置 (親機) と無線端末装置群 (子機) とで新しいネットワークを形成している間に、SSIDで構成された元のネットワークに無線端末装置 (親機) と同じ IP アドレスを割り振った無線端末装置が参加している場合に、無線端末装置 (親機) が、SSIDを再度使用して元のネットワークに再参加する際に、改めて IP アドレスを振り直すことにより、IP アドレスの衝突をさけ、円滑に元のネットワークに復帰できる無線 LAN システムを提供するものである。

【 0 0 6 9 】

図 1 9 は、第 7 の実施形態における無線 LAN システムの構成を示す図である。図 1 9 において、1 9 0 1 は第 6 の実施形態によりSSID2のデータ通信チャネルを切断し、SSID1のビーコンを発信している状態の無線端末装置である。1 9 0 2 は無線端末装置 1 9 0 1 がSSID2のデータ通信チャネルを構築している間に、無線端末装置 1 0 4、1 0 5、1 9 0 3 で構築したSSID1のデータ通信チャネルである。

【 0 0 7 0 】

尚、無線端末装置 1 9 0 3 は、無線端末装置 1 9 0 1 と同一の IP アドレス (192.168.0.2) を取得し、1 9 0 2 のアドホックネットワークに参加しているものとする。

【 0 0 7 1 】

ここで、第 7 の実施形態におけるアドホックネットワークを構築する処理を、図 2 0 を用いて説明する。

【 0 0 7 2 】

図 2 0 は、第 7 の実施形態におけるシーケンスを示す図である。第 6 の実施形態で説明したように、データ通信可能な状態で (1 9 0 1 ~ 1 9 0 7)、無線端末装置 1 9 0 1 がアドホックネットワークを切断する (1 9 0 8)。そして、元のSSID1のビーコンを発信し、元のアドホックネットワークに復帰しようとしたとき、無線端末装置 1 9 0 1 と同一の IP アドレスを所有しているジョイナーとして機能する無線端末装置 1 9 0 3 が復帰先のアドホックネットワークに存在する場合、無線端末装置 1 9 0 1 は一旦自分の IP アドレスをクリアし、再度新しい IP アドレスを取得する。このとき、新しい IP アドレスはランダムでも良いし、元の IP アドレスから一定の値をインクリメントする方法やデクリメントする方法でも良い。

【 0 0 7 3 】

そして、新しい IP アドレスを取得すると、元のSSID1を含むビーコンを無線端末装置群 1 0 4、1 0 5、1 9 0 3 に対して発信する (1 9 0 9)。

【 0 0 7 4 】

第 7 の実施形態によれば、元のネットワークに再参加するときに、IP アドレスの衝突を防ぐことが可能となる。

【 0 0 7 5 】

尚、本発明は複数の機器（例えば、ホストコンピュータ、インターフェース機器、リーダー、プリンタなど）から構成されるシステムに適用しても、1つの機器からなる装置（例えば、複写機、ファクシミリ装置など）に適用しても良い。

【 0 0 7 6 】

また、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記録媒体を、システム或いは装置に供給し、そのシステム或いは装置のコンピュータ（CPU 若しくは MPU）が記録媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。

10

【 0 0 7 7 】

この場合、記録媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記録媒体は本発明を構成することになる。

【 0 0 7 8 】

このプログラムコードを供給するための記録媒体としては、例えばフロッピー（登録商標）ディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、CD-R、磁気テープ、不揮発性のメモリカード、ROMなどを用いることができる。

20

【 0 0 7 9 】

また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働している OS（オペレーティングシステム）などが実際の処理の一部又は全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【 0 0 8 0 】

更に、記録媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わる CPU などが実際の処理の一部又は全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

30

【 図面の簡単な説明 】

【 0 0 8 1 】

【 図 1 】 第 1 の実施形態における無線 LAN システムの構成例を示す図である。

【 図 2 】 無線端末装置間における接続時のシーケンスを示す図である。

【 図 3 】 第 1 の実施形態における接続時の処理を示すフローチャートである。

【 図 4 】 第 1 の実施形態における無線端末装置 102 の概略構成を示すブロック図である。

。

【 図 5 】 第 2 の実施形態における接続時の手順を示すフローチャートである。

40

【 図 6 】 第 2 の実施形態における無線端末装置 102 の概略構成を示すブロック図である。

。

【 図 7 】 第 3 の実施形態における無線端末装置間のシーケンスを示す図である。

【 図 8 】 第 3 の実施形態におけるデータ通信可能後の処理を示すフローチャートである。

【 図 9 】 第 3 の実施形態における無線端末装置 102 の概略構成を示すブロック図である。

。

【 図 10 】 第 4 の実施形態における無線端末装置間のシーケンスを示す図である。

【 図 11 】 第 4 の実施形態における処理を示すフローチャートである。

【 図 12 】 第 4 の実施形態における無線端末装置 102 の概略構成を示すブロック図である。

50

【図 1 3】第 5 の実施形態における無線 LAN システムの構成例を示す図である。

【図 1 4】第 5 の実施形態におけるシーケンスを示す図である。

【図 1 5】第 5 の実施形態における処理を示すフローチャートである。

【図 1 6】第 6 の実施形態における無線 LAN システムの構成例を示す図である。

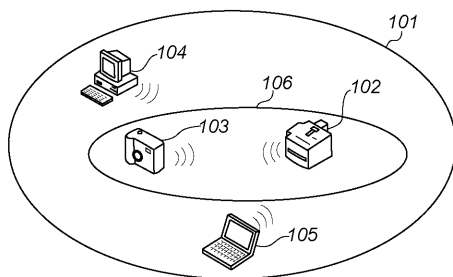
【図 1 7】第 6 の実施形態における無線端末装置のシーケンスを示す図である。

【図 1 8】第 6 の実施形態における無線端末装置の他のシーケンスを示す図である。

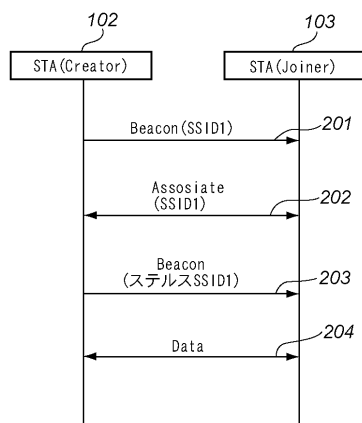
【図 1 9】第 7 の実施形態における無線 LAN システムの構成を示す図である。

【図 2 0】第 7 の実施形態におけるシーケンスを示す図である。

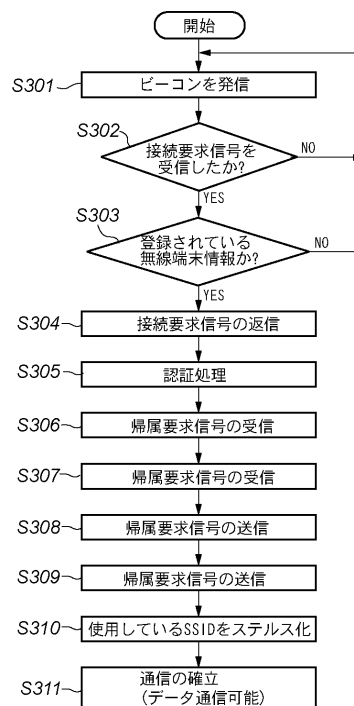
【図 1】



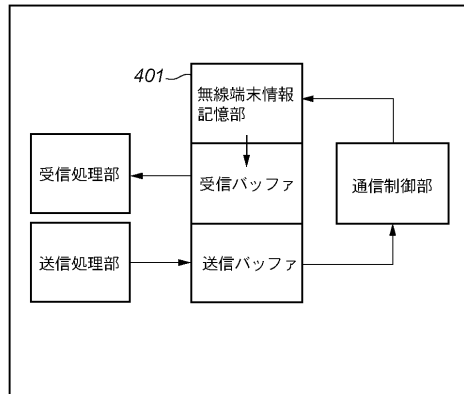
【図 2】



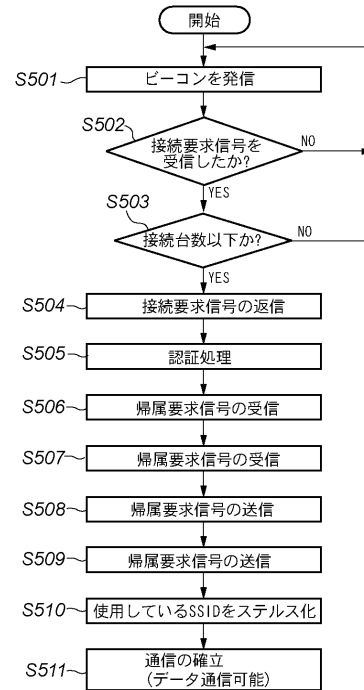
【図 3】



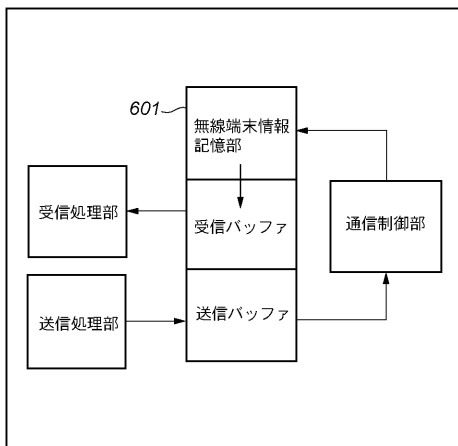
【図 4】



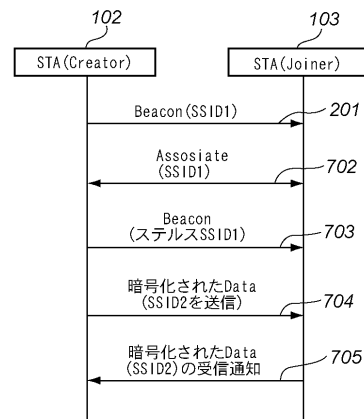
【図 5】



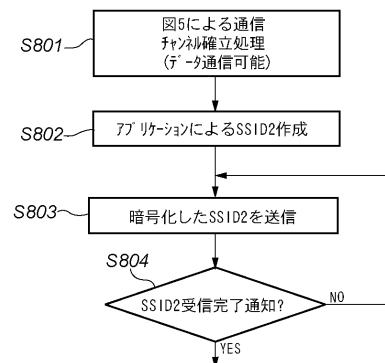
【図 6】



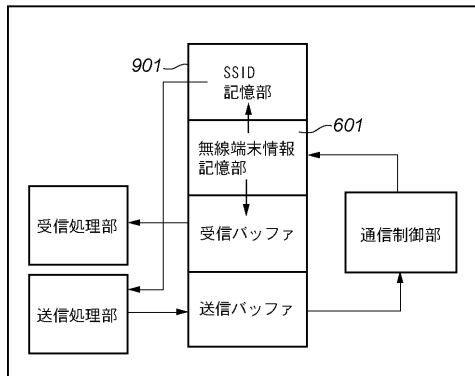
【図 7】



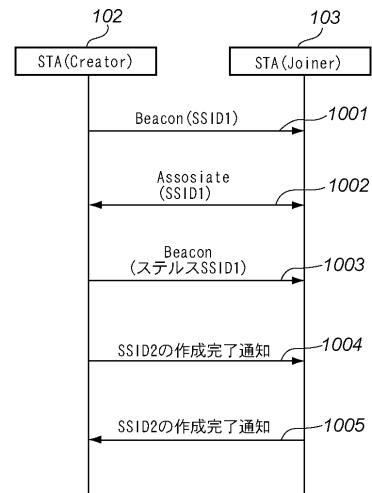
【図 8】



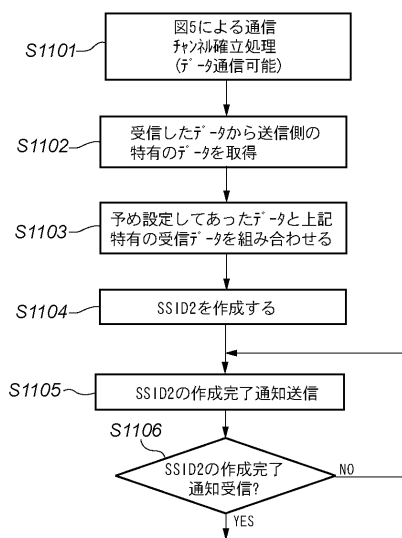
【図 9】



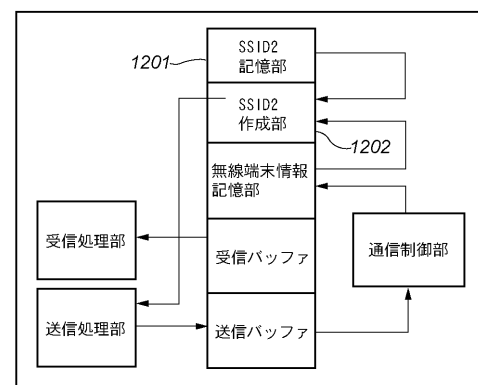
【図 10】



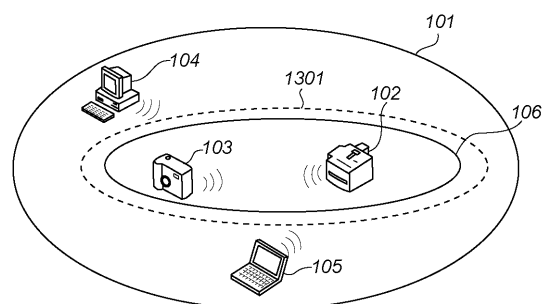
【図 11】



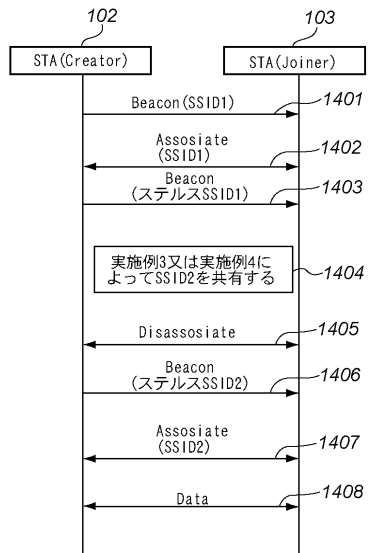
【図 12】



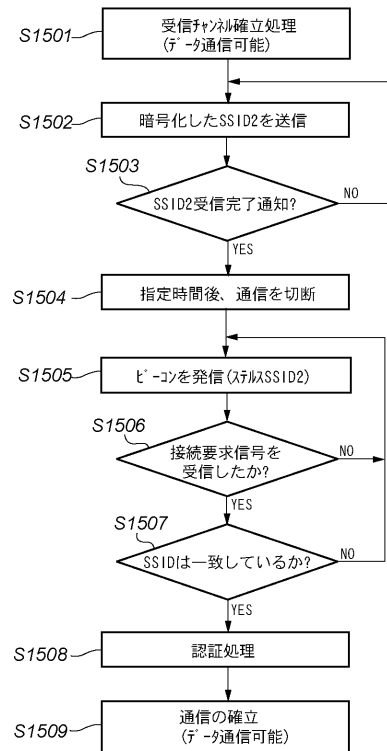
【図 13】



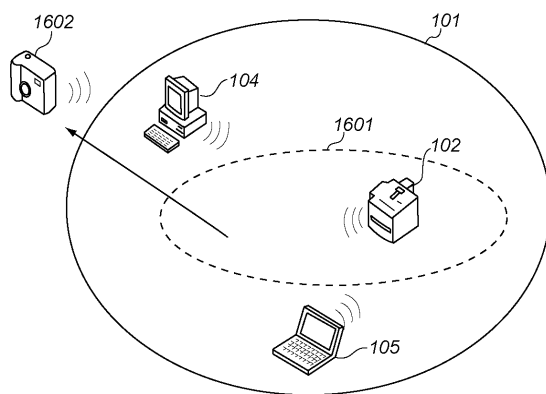
【図 14】



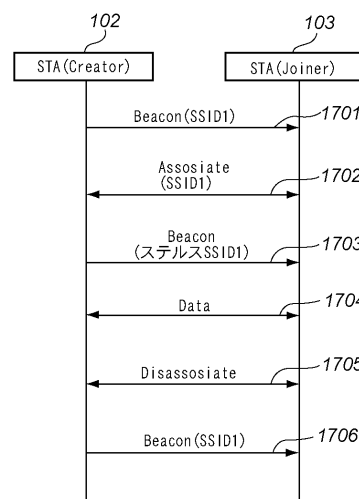
【図 15】



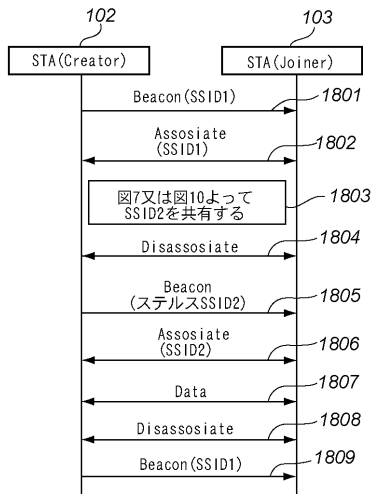
【図 16】



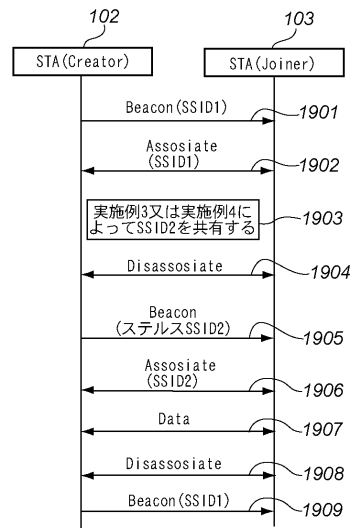
【図 17】



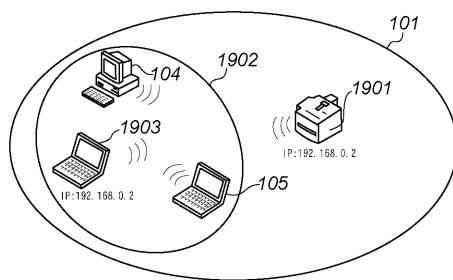
【図 18】



【図 20】



【図 19】



フロントページの続き

(72)発明者 林 健一郎

東京都大田区下丸子3丁目30番2号 キヤノン株式会社内

(72)発明者 後藤 史英

東京都大田区下丸子3丁目30番2号 キヤノン株式会社内

Fターム(参考) 5K033 AA08 CC01 DA01 DA19 DB12 EA03 EA05 EB03 EC03